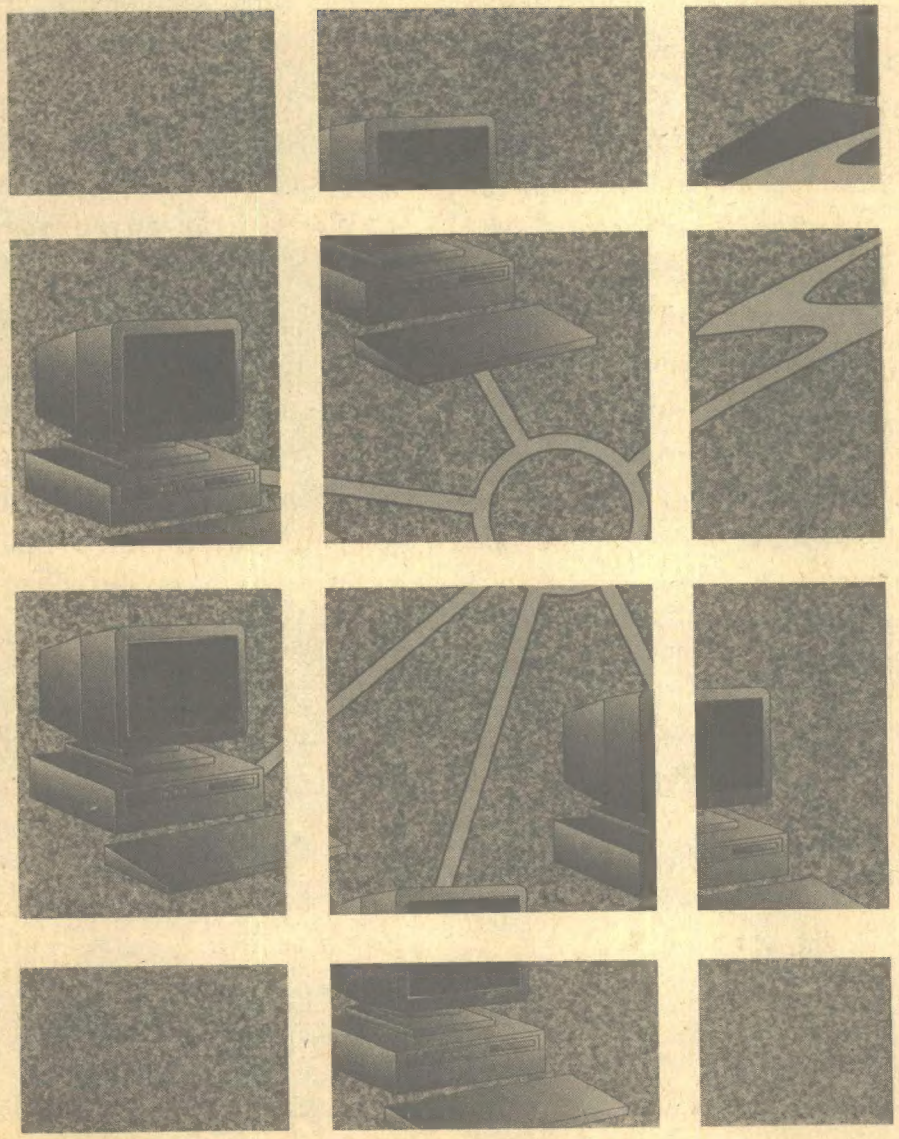
บทความพิเศษ

COMPUTER SECURITY

สิทธิพงศ์ จันทร์แสงอรุณ

การป้องกัน ระบบเครือข่าย

ระวังให้ดีคุณดูแล
และป้องกันระบบเครือข่าย
ของคุณดีหรือยัง มิฉะนั้น!



คุณเคยสังเกตบ้างไหมว่า เมื่อคุณเข้าไปใช้ระบบเครือข่ายหรือพยายามเข้าไปใช้แอพพลิเคชันบางตัว คุณจะต้องผ่านระบบตรวจสอบต่าง ๆ ตั้งแต่การป้อนกัน ID และ password ของตนเองให้ถูกต้อง จึงจะเข้าระบบเครือข่ายหรือแอพพลิเคชันนั้น ๆ ได้ นี่เป็นการป้องกันผู้ใช้ ที่ไม่สมควรจะได้ใช้ระบบนั่นเองเพราะผู้ที่ไม่มี ID หรือไม่อนุญาตให้มี ID จะไม่สามารถเข้าไปใช้ระบบได้ แต่ในบางระบบหรือบางแอพพลิเคชันก็จะยอมให้ใครก็ตามเข้ามาใช้ระบบ สามารถใช้ระบบได้ทันทีโดยไม่ต้องมี ID เลย

การป้องกันระบบจากบุคคลที่ไม่พึงประสงค์มีมากมายหลายวิธี วิธีของการใช้ ID และ password ที่ได้กล่าวมาข้างต้นเป็นเพียงการป้องกันระบบจากด้านผู้ใช้งานเท่านั้น การป้องกันระบบเครือข่ายหรือแม้แต่ระบบเมน-เฟรมมีความยุ่งยากซับซ้อนมาก ถ้าคุณสนใจถึงวิธีการป้องกันระบบที่ใช้กันอยู่มากมายในตลาด การใช้งานชนิดและประเภทของระบบป้องกันต่าง ๆ บทความนี้คงเป็นบทความที่คุณสนใจเป็นแน่

ในบทความนี้เราจะเอ่ยถึงว่าทำไมคุณจึงต้องการป้องกันระบบของคุณจากบุคคลภายนอก มาตรฐานการป้องกันระบบชนิดต่าง ๆ การแบ่งแยกชนิดของการป้องกันทั้งในด้านซอฟต์แวร์และ

ฮาร์ดแวร์ ความเสียหายชนิดต่าง ๆ ที่อาจเกิดขึ้นกับระบบและข้อมูลในระบบของคุณ การป้องกันไวรัส ฯลฯ

ทำไมต้องมีการป้องกันระบบ

คุณก็คงจะรู้อยู่แล้วว่าในระบบเครือข่ายหรือเมนเฟรมเองมีข้อมูลอยู่มากมาย ทั้งเป็นประโยชน์แก่บุคคลใดบุคคลหนึ่งหรือมีประโยชน์ทางการค้าต่อบริษัทคู่แข่งของคุณเอง คุณคงไม่อยากให้ผู้ใช้มาขโมยข้อมูลที่คุณหรือสถานศึกษาของคุณ หรือบริษัทของคุณหามาได้ด้วยความยากลำบาก หรือบุคคลอื่นใดเข้ามาเพื่อทำลายข้อมูลเหล่านั้น การป้องกันระบบจากผู้ใช้ที่ไม่ได้รับอนุญาตให้ใช้จึงมีความสำคัญมาก ไม่เพียงแต่ป้องกันบุคคลภายนอกเท่านั้น ระบบการป้องกันที่ดีสามารถป้องกันผู้ใช้ที่ไม่มีความระวัง เข้าไปทำลายข้อมูลหรือเปลี่ยนแปลงข้อมูลโดยไม่ตั้งใจได้ด้วย การป้องกันที่ดีจะไม่เป็นเพียงการป้องกันไม่ให้บุคคลใดบุคคลหนึ่งเข้ามาในระบบเท่านั้น มันจะต้องป้องกันตัวระบบเองจากสาเหตุอื่น ๆ ด้วยเช่น ไฟไหม้ ไฟฟ้าลัดวงจร น้ำท่วม ฮาร์ดแวร์ส่วนหนึ่งส่วนใดชำรุด ฯลฯ ทั้งยังต้องมีระบบฉุกเฉินเพื่อใช้แก้ไขในกรณีที่มีเหตุการณ์ที่ทำให้ระบบเสียหายได้

จากการศึกษาและสอบถามไปยังบริษัท และสถานศึกษามากมายพบว่ายิ่งระบบของหน่วยงานหรือสถานศึกษามีขนาดใหญ่เท่าใด ก็จะให้ความสำคัญของการป้องกันมากขึ้นเท่านั้น เพราะเมื่อมีผู้ใช้ระบบมากเท่าใด การควบคุมดูแลก็จะยากขึ้นเท่านั้น บางบริษัทหรือหน่วยงานถึงกับยอมลงทุนในอุปกรณ์ทั้งฮาร์ดแวร์และซอฟต์แวร์ป้องกันระบบที่มีราคามากถึง 25% ของราคาระบบทั้งหมดทีเดียว (ปกติจะอยู่ในราว ๆ 5-10 เปอร์เซ็นต์เท่านั้น)

สาเหตุที่ทำให้เกิดความเสียหายชนิดต่าง ๆ

สาเหตุต่าง ๆ ที่อาจทำให้เกิดความเสียหายแก่ระบบ ตั้งแต่ทำให้ข้อมูลบางอย่างเกิดความเสียหายไปจนถึงการทำให้ระบบทั้งหมดหยุดทำงานได้ ตารางที่ 1 แสดงถึงสาเหตุต่าง ๆ ที่อาจทำให้เกิดความเสียหายแก่ระบบของคุณได้

คุณจะเห็นได้ว่าส่วนใหญ่แล้วความเสียหายจะเกิดขึ้นจากอุบัติเหตุและความผิดพลาดของผู้ใช้ระบบและผู้ควบคุมระบบเป็นส่วนใหญ่ (35%) และรองลงมาก็เป็นความเสียหายเมื่อมีบุคคลอื่นที่สามารถเข้ามาใช้ระบบได้ (21%) ซึ่งบุคคลเหล่านั้นอาจทำการคัดลอกเอาข้อมูลของคุณออกไปขายให้แก่ที่อื่นหรือทำลายข้อมูลของคุณได้ การที่ผู้ใช้ระบบไม่ซื่อสัตย์ก็เป็นอีกสาเหตุหนึ่ง (9%) คุณจึงไม่ควรให้ผู้ใช้เหล่านี้เข้าไปอ่านข้อมูลใด ๆ นอกเหนือจากความรับผิดชอบของพวกเขา ระบบฮาร์ดแวร์หรือซอฟต์แวร์เสียหาย (7%) อาจเกิดจากอายุการใช้งานของฮาร์ดแวร์นั้น ๆ หรือการควบคุมอุณหภูมิและความชื้นที่ไม่เหมาะสม ไฟฟ้า surge ไฟไหม้ ฟ้าผ่าล้วนอาจเกิดขึ้นได้ถ้าไม่มีระบบป้องกันที่ดี เช่นมียูพีเอสเพื่อป้องกันไฟตกหรือไฟเกิน มีอุปกรณ์ตรวจจับควันและความร้อนที่ดี หรือมีระบบสายล่อไฟที่ดี

สาเหตุต่าง ๆ ที่กล่าวมาข้างต้นนี้อาจทำความเสียหายแก่ระบบของคุณคิดเป็นเงินได้แตกต่างกันอย่างมากขึ้นอยู่กับปัจจัยหลายอย่าง อุบัติเหตุหรือความผิดพลาดของผู้ใช้หรือผู้ควบคุมระบบอาจทำความเสียหายเล็กน้อยจนถึงความเสียหายมากมายได้ และสาเหตุจากไฟไหม้อาจจะทำความเสียหายระบบทั้งหมดของคุณเลยทีเดียว ดังนั้นคุณควรที่จะหาทางป้องกันระบบของคุณจากทุก ๆ สาเหตุที่อาจเกิดขึ้น

จากตารางที่ 1 เป็นเพียงสาเหตุที่ทำให้เกิดความเสียหายแก่หน่วยงานต่าง ๆ จากประสพการณ์ของผู้เขียนที่เจอมา ดังนั้นถ้าคุณมีระบบการป้องกันที่ดี เช่น มีวิธีการอย่างเด่นชัดเพื่อให้ผู้ใช้และผู้ควบคุมระบบได้ทำตาม การเกิดขึ้น

สาเหตุต่าง ๆ	การเกิด
อุบัติเหตุและความผิดพลาดของคน	35%
บุคคลอื่นเข้ามาในระบบ	21%
ไวรัส	12%
ผู้ใช้ระบบไม่ซื่อสัตย์	9%
ฮาร์ดแวร์หรือซอฟต์แวร์เสียหาย	7%
ไฟฟ้า Surge	6%
ไฟไหม้	3%
ฟ้าผ่า	2%
อื่น ๆ	5%

ตารางที่ 1
ความเสียหายที่อาจเกิดขึ้นในระบบ

ของข้อผิดพลาดก็จะน้อยลงทันที หรือการตรวจสอบไวรัสกับแผ่นดิสค์ทุกแผ่นก่อนนำมาใช้ในระบบก็สามารถกำจัดปัญหาการติดไวรัสได้เกือบหนึ่งร้อยเปอร์เซ็นต์เลยทีเดียว

มาตรฐานการป้องกันระบบ

ในปี 1983 หน่วยงานป้องกันระบบคอมพิวเตอร์หรือ Department of Defense Computer Security ในสหรัฐอเมริกาได้ออกหนังสือชื่อ Trusted Computer Security Evaluation Criteria (TCSEC) หรือเรียกกันติดปากว่าหนังสือปกส้มเพราะว่าหนังสือเล่มนี้มีปกเป็นสีส้มสะดุดตามาก หนังสือเล่มนี้จะบอกแนวทางของการป้องกันสำหรับผู้สร้างและผู้ซื้อระบบ ผู้ที่ซื้อระบบมาใช้สามารถใช้หนังสือเล่มนี้เป็นการเปรียบเทียบถึงระบบป้องกันของตนเอง ซึ่งจะบอกว่าระบบที่ตนจะซื้อมีระบบป้องกันเป็นอย่างไร

หนังสือปกส้มจะกล่าวถึงการป้องกันข้อมูลในระบบคอมพิวเตอร์ที่มีผู้ใช้มากกว่าหนึ่ง และใช้สำหรับเปรียบเทียบระบบดาต้าเบสด้วย ซึ่งหลักใหญ่จริง ๆ ต้องการเขียนขึ้นสำหรับผู้ที่ต้องการทำระบบให้รัฐบาลสหรัฐอเมริกาและทางการทหารของสหรัฐเท่านั้น แต่ในปีหลัง ๆ มาหนังสือปกส้มก็เข้ามามีบทบาทในธุรกิจทางด้านระบบเครือข่ายในตลาดมากขึ้นเพราะความเป็นมาตรฐานของมันได้รับการยอมรับอย่างกว้างขวาง และผู้สร้างระบบก็พยายามสร้างระบบของตัวเองโดยใช้การวัดระดับการป้องกันตามแบบในหนังสือปกส้มด้วย ระบบใดต้องการรู้ว่าอยู่ในระดับใด มันจะต้องผ่านการทดสอบที่ยาก กินเวลานาน และมีราคาแพงมากด้วย

ประเภท/ระดับของการป้องกัน	ระบบการป้องกัน
ประเภท A ● ระดับ A1	เป็นการป้องกันที่ดีที่สุด ใช้วิธีการป้องกันแบบตรวจสอบ (verified protection) เหมาะกับคอมพิวเตอร์ทางการทหาร
ประเภท B ● ระดับ B3 ● ระดับ B2 ● ระดับ B1	เป็นการป้องกันในระบบการควบคุมการใช้ของผู้ใช้หรือ mandatory access control (MAC)
ประเภท C ● ระดับ C2 ● ระดับ C1	เป็นการป้องกันแบบ discretionary access control (DAC) ซึ่งเป็นการป้องกันโดยผู้เป็นเจ้าของไฟล์ให้สิทธิ์แก่ผู้อื่นในการใช้ไฟล์นั้น ๆ ระบบส่วนใหญ่จะอยู่ในประเภทนี้
ประเภท D ● ระดับ D	เป็นการป้องกันที่ต่ำที่สุด มีไว้เพื่อบอกถึงระบบที่ไม่ผ่านการทดสอบ

ตารางที่ 2 ตารางแสดงประเภทและระดับของระบบป้องกัน

หนังสือปกส้มได้แบ่งระดับการป้องกันเอาไว้ทั้งหมด 7 ระดับโดยมีระดับต่ำสุดเป็นระดับที่เรียกว่าระดับ D ซึ่งจะให้กับระบบที่ไม่ผ่านระบบป้องกันอะไรเลย ถ้าคุณส่งที่รองเม้าส์ของคุณเข้าไปวัดระดับการป้องกันที่รองเม้าส์ของคุณก็จะได้ระดับ D แน่นอน

ระดับทั้งเจ็ดนี้จะถูกแบ่งออกเป็น 4 ประเภทแสดงไว้ในตารางที่ 2

ประเภทการป้องกันจากน้อยไปมากคือจาก D ไปจนถึง A ในแต่ละประเภทยังแบ่งออกเป็นระดับต่าง ๆ ระดับที่แสดงตัวเลขที่สูงกว่าจะมีการป้องกันที่ดีกว่า ตัวอย่างเช่นในประเภท B จะมีระดับ B3 เป็นระบบการป้องกันที่สูงกว่าระดับ B2 และ B1

ประเภท D

อย่างที่กล่าวไว้ข้างต้น ระดับ D จะเป็นระดับและประเภทของระบบที่ไม่ผ่านการทดสอบ ซึ่งไม่สมควรที่จะได้รับระดับการป้องกันในระดับอื่น ๆ ซึ่งอาจจะหมายความว่าระบบนั้นไม่มีระบบป้องกันอะไรเลยก็ได้

ประเภท C

เป็นระบบการป้องกันแบบ discretionary access control (DAC) ซึ่งเป็นการป้องกันที่ผู้เป็นเจ้าของไฟล์ให้สิทธิ์ในการใช้ไฟล์แก่ผู้อื่นได้ จะใช้ร่วมกับความสามารถในการ audit สำหรับการกระทำต่าง ๆ ของผู้ให้และผู้ใช้สิทธิ์ด้วย

ระดับ C1 : discretionary security protection

เป็นระดับการป้องกันของระบบเริ่มต้น ผู้ใช้สามารถป้องกันไม่ให้ไฟล์ของตัวเขาเองจากการถูกอ่าน ถูกแก้ไข และถูกทำลายโดยผู้ใช้คนอื่น ๆ ระบบทั้งหมดจะต้องป้องกันด้วยการใช้ pass-

word และที่ ๆ เก็บ password จะต้องไม่มีใครเข้าไปยุ่งเกี่ยวหรือเข้าไปดูได้ ระบบที่จะได้ระดับการป้องกัน C1 มันจะต้องผ่านการทดสอบของระบบและมีเอกสารประกอบทุกขั้นตอน ระบบที่ขายกันอยู่ในตลาดส่วนใหญ่จะได้รับระดับการป้องกันชนิดนี้ ระบบปฏิบัติการ UNIX System V เข้าใกล้ระดับนี้มากโดยที่ไม่จำเป็นต้องมีการแก้ไขใด ๆ เลย

ระบบ trusted computing base (TCB) ของระดับ C1 เป็นระบบที่ยอมรับกัน โดยการแยกผู้ใช้ออกจากข้อมูลทั้งหลาย และมีการจัดระบบการป้องกันโดยการให้สิทธิ์ในการเข้าถึงข้อมูลตามแต่ที่ผู้ใช้จำเป็น ระบบนี้เป็นระบบที่เหมาะกับผู้ใช้ที่มีระดับความต้องการในการเข้าถึงข้อมูลเท่า ๆ กัน

ระดับ C2 : controlled access protection

ระบบการป้องกันระดับ C2 จะสามารถยอมหรือปฏิเสธการเข้าถึงของข้อมูลจากผู้ใช้ สิ่งที่ทำได้มากกว่าระดับ C1 ก็คือความสามารถในการป้องกันไม่ให้ผู้ใช้คนอื่นอ่านข้อมูลที่อยู่ในหน่วยความจำของผู้ใช้ได้ หรือสามารถทำให้ไฟล์ที่ผู้ใช้คนอื่นได้ลบทิ้งไปแล้วกลับมาใช้ใหม่ได้ ระบบในระดับ C2 จะต้องมีการบันทึกการเข้าระบบทุกครั้ง ไฟล์ทุกไฟล์ที่ถูกเปิดอ่าน การสร้างหรือลบไฟล์ ไม่ว่าผู้ใช้จะเป็นผู้ใช้ธรรมดาหรือผู้ควบคุมระบบ (system administrator) ไม่มีใครได้รับการยกเว้น

ระบบการป้องกันในระดับ C2 นี้จะทำให้ผู้ใช้รับผิดชอบต่อการกระทำของตนเองผ่านการเข้าระบบ ความสามารถในการบันทึกการกระทำต่าง ๆ (auditing) และการแยกรีซอร์สต่าง ๆ ออกมา

ตัวอย่างของระบบปฏิบัติการที่อยู่ในระดับ C2 คือ UNIX System V Release 4.2 และ Microsoft Windows NT ซึ่งหมายความว่าเวอร์กสเตชันตัวใดที่ใช้ระบบปฏิบัติการเหล่านี้ ผู้ใช้จะต้องทำการเข้าระบบโดยมี ID และ password

ประเภท B

ระบบประเภทนี้จะใช้วิธีการ sensitivity labels คือการระบุระดับความสำคัญไว้ที่ดาต้าสตรักเจอร์ต่าง ๆ ในระบบ ทุก ๆ ออปเจ็กต์ในระบบจะถูกระบุระดับความสำคัญไว้ คล้าย ๆ กับการบอกว่า เป็นความลับสุดยอด เป็นความลับ หรือลับเฉพาะ แต่ละออปเจ็กต์หรือไฟล์จะมีการระบุค่าความสำคัญได้ค่าเดียวเท่านั้น และผู้ใช้สามารถอ่านออปเจ็กต์หรือไฟล์นั้น ๆ ได้ก็ต่อเมื่อผู้ใช้มีระดับในการอ่านไฟล์หรือออปเจ็กต์ระดับที่เท่ากับ หรือเหนือกว่าระดับที่ถูกกำหนดไว้ในออปเจ็กต์หรือไฟล์เท่านั้น

ระดับ B1 : labeled security protection

เป็นการป้องกันโดยการระบุค่าทุก ๆ ออปเจ็กต์ (ไฟล์ โปรแกรม การพิมพ์ ฯลฯ) ในระบบจะถูกระบุค่าความสำคัญ และผู้ใช้แต่ละคนจะถูกระบุค่าการใช้ (clearance level) ซึ่งเป็นการกำหนดถึงการเข้าถึงข้อมูลที่มีค่าที่ผู้ใช้นั้น ๆ จะทำได้

ทุก ๆ ไฟล์ในระบบระดับ B1 หรือมากกว่าจะถูกจัดระดับตามข้อมูลของมัน (เช่น ข้อมูลเงินเดือน การรับใบสั่งของ หรืออื่น ๆ) ผู้ใช้จะถูกจำกัดการเข้าอ่านข้อมูลตามแต่ที่ผู้ใช้คนนั้นรับผิดชอบเท่านั้น หรือก็คือไฟล์ในระดับที่เขาเข้าได้ตามค่าการใช้ที่ถูกระบุไว้ที่ผู้ใช้เท่านั้น การเปลี่ยนแปลงของระดับค่าการใช้จะถูกควบคุมอยู่ตลอดเวลา

ระดับ B1 จะรวมเอาความสามารถของระดับ C2 ทุกอย่างบวกกับความสามารถของการระบุค่าความสำคัญของออปเจ็กต์ การกำหนดการเข้าหาข้อมูล การกำหนดค่าการใช้ ตัวอย่างระบบในระดับ B1 คือ ระบบเมนเฟรมของ IBM ที่ชื่อว่า ระบบปฏิบัติการ MVS ซึ่งใช้ร่วมกับซอฟต์แวร์ป้องกันระบบตัวหนึ่งตัวใดในสามชนิดคือ RACF (resource access control facility) ของไอบีเอ็มหรือหนึ่งในสองซอฟต์แวร์ของบริษัท Computer Associates คือ ACF2 หรือ TopSecret

ระดับ B2 : structured protection

เป็นการป้องกันข้อมูลโดยการแบ่งมันออกเป็นประเภทต่าง ๆ ผู้ใช้ก็ต้องอยู่ในประเภทนั้น ๆ จึงจะสามารถใช้ข้อมูลเหล่านั้นได้ ในระดับการป้องกัน B2 นี้จะใช้การป้องกันทั้งหมดของระดับ B1 รวมไปจนถึงระบบการป้องกันในระบบ ADP (automatic data processing) รวมไปถึงการส่งผ่านข้อมูลออกไปที่อื่นโดยผ่าน communication channal ด้วย ระบบการป้องกันของระดับ B2 แทบจะป้องกันการแทรกซึมถึงข้อมูลต่าง ๆ ได้ทั้งหมด

ระดับ B3 : security domains

เป็นการป้องกันที่มีการตรวจสอบการเข้าถึงทุก ๆ ไฟล์ ทุก ๆ ออปเจ็กต์ และข้อมูลจะถูกเก็บอยู่ในที่ ๆ ปลอดภัย ซึ่งจะมีขนาดเล็กพอที่จะนำไปทดสอบ ถ้าไม่มีระดับ B3 ระบบยูนิกซ์ส่วนใหญ่ก็จะตกอยู่ในระดับ B1 เท่านั้น ในระดับนี้มีการรองรับการทำงานของ

security administrator มีความสามารถในการทำ audit สูง ซึ่งรวมไปถึงการส่งสัญญาณเหตุการณ์ที่ผู้ใช้พยายามเข้าถึงข้อมูลที่ไม่สมควรเข้าไปให้บุคคลที่รับผิดชอบได้ด้วย ระบบในระดับ B3 ยากที่ผู้ใดจะเข้าถึงระบบได้ถ้าไม่ได้รับอนุญาต

ประเภท A

เป็นการป้องกันแบบ verified protection หรือการป้องกันแบบตรวจสอบ ซึ่งเป็นการทำให้แน่ใจว่าได้รวมเอาระบบการป้องกันแบบ mandatory และ discretionary ไว้ในระบบ ที่ป้องกันการเข้าถึงข้อมูลลับที่มีการระบุค่าความสำคัญของข้อมูลที่ถูกเก็บหรือทำงานอยู่โดยระบบ ระดับการป้องกันในประเภทนี้มีอยู่ระดับเดียวคือ ระดับ A1

ระดับ A1 : verified protection

เป็นระบบที่ถูกสร้างขึ้นมาเฉพาะเพื่อให้ได้ระบบการป้องกันอย่างจริงจัง เป็นระบบที่มีการควบคุมการป้องกันในระดับของซอฟต์แวร์ที่ใช้กับระบบจากจุดที่สร้างขึ้นมาในโรงงานจนถึงระดับผู้ใช้งานเลยทีเดียว เป็นการแน่ใจว่าการป้องกันที่ทำมาจากโรงงานจะได้รับการป้องกันอย่างเต็มที่โดยผู้ใช้

ระบบการป้องกันระดับ A1 จะเหมือนกับการป้องกันระดับ B3 ทุกอย่าง เพียงแต่มันจะมีความเที่ยงตรงสูงกว่าโดยใช้เทคนิคการตรวจสอบหลายหน และจะส่งผลให้มีความเที่ยงตรงสูงเป็นอย่างมาก เป็นการสร้างโดยการเริ่มต้นการออกแบบด้วยโมเดลการป้องกันที่เป็นมาตรฐานและ formal top-level specification (FTLS) คือการคำนวน

ที่รองรับระบบป้องกัน จำเป็นต้องมีผู้ควบคุมระบบการป้องกันหรือ system administrator ด้วย

ระดับการป้องกันระบบที่นิยมใช้กันในระบบเครือข่ายก็คือ ระดับ C2 แต่ถ้าใช้ในระบบเมนเฟรมขึ้นไป จะนิยมใช้ระบบการป้องกันในระดับ B1 มากกว่า ครั้งหน้าที่คุณจะพิจารณาระบบปฏิบัติงานเน็ตเวอร์ก คุณก็รู้ได้เลยว่าคุณต้องพิจารณาระบบที่มีระดับการป้องกันเท่ากับ C2 หรือมากกว่าเท่านั้นเพื่อป้องกันระบบเครือข่ายของคุณเอง

การป้องกันระบบทางด้านซอฟต์แวร์

การที่คุณซื้อระบบปฏิบัติการที่มีระดับการป้องกันสูง ๆ มาใช้ก็ไม่ได้หมายความว่าคุณสามารถป้องกันความเสียหายของข้อมูลได้ ถ้าคุณไม่กำหนดข้อป้องกันของระบบที่คุณได้มาอย่างถูกต้อง ซอฟต์แวร์ของระบบที่คุณซื้อมาอาจมีความสามารถที่ให้คุณเลือกใช้ระบบป้องกันต่าง ๆ ตามที่คุณต้องการ คุณจะต้องใช้ฟังก์ชันเหล่านั้นมาควบคุมระบบ ตัวอย่างของฟังก์ชันการป้องกันการใช้ ID และ password ที่คุณควรจะใช้คือ

- กำหนดความยาวต่ำสุดของ password เพื่อป้องกัน password ที่ง่ายแก่การคาดเดา
- กำหนดการหมดอายุของ password เพื่อไม่ให้ผู้ใช้ใช้ได้นานเกินไป
- กำหนดไม่ให้ผู้ใช้ใช้ password ซ้ำเป็นจำนวนที่มากกว่าสี่ตัว เพื่อป้องกันไม่ให้ผู้ใช้ใช้ password ซ้ำไปซ้ำมาเพียงไม่กี่ตัว
- กำหนดจำนวนครั้งการพยายามเข้าระบบแต่ป้อน password ไม่ถูกต้องก่อนที่ระบบจะตัดสิทธิ์การใช้ ID นั้นเพื่อป้องกันการลองเข้าระบบ
- การกำหนดให้ระบบแสดงวันและเวลาของการใช้งานที่ผู้ใช้ใช้ระบบเป็นครั้งสุดท้าย เพื่อให้ผู้ใช้สามารถตรวจสอบได้ว่ามีใครแอบใช้งาน ID ของตนเองหรือไม่
- การกำหนดเวลาเพื่อให้ระบบ logout ผู้ใช้ออกไป หากผู้ใช้ไม่มีการใช้ระบบเป็นระยะเวลาหนึ่ง

การ encrypt ข้อมูลที่วิ่งไปมาในระบบก็เป็นการป้องกันที่นิยมใช้กันอย่างมาก ในระบบเครือข่ายส่วนใหญ่จะมีการทำ encryption ก่อนที่เวอร์กสเตชันหนึ่ง ๆ จะทำการส่งผ่านข้อมูลไปมาในระบบ เพื่อเป็นการป้องกันระบบจากผู้ไม่หวังดีที่ใช้วิธีการขโมยต่อเชื่อมเข้ากับระบบของเราและดึงเอาข้อมูลที่วิ่งอยู่ในระบบไป แต่ในระบบเครือข่ายบางชนิดของคุณจะต้องเข้าไปกำหนดพารามิเตอร์บางตัวเพื่อให้มันทำ encryption การทำ encryption ในระบบเครือข่ายนิยมทำกันในสามระดับคือ ระดับ data link layer, ระดับ transport layer, และในระดับ application layer รูปที่ 1 จะแสดงให้เห็นถึงการป้องกันในระดับต่าง ๆ ใน IS0 OSI Model :

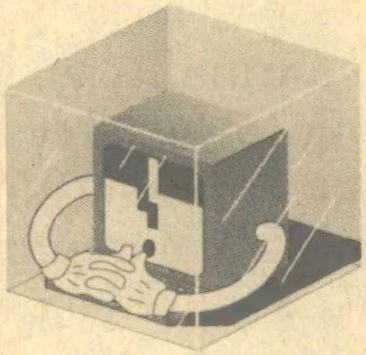
ถ้าคุณเลือกใช้การป้องกันในระดับ datalink layer เวอร์กสเตชันตัวส่งจะ encrypt ข้อมูลใน layer ที่สองและทำการส่งข้อมูลนั้น ๆ ข้ามระบบเครือข่ายไป ขณะที่ข้อมูลผ่านไปยังเวอร์กสเตชันตัวอื่น มันจะถูก decrypt และ encrypt อีกครั้งเพื่อส่งต่อไปยังเครื่องต่อไป เมื่อข้อมูลมาถึงเวอร์กสเตชันที่รับข้อมูล มันก็จะ decrypt ข้อมูลออกมาและส่งข้อมูลต่อไปยัง layer ข้างบนต่อไป การทำงานของการ encrypt ที่ระดับ datalink นี้อาจทำให้ประสิทธิภาพของระบบตกลง และข้อเสียอีกอย่างก็คือข้อมูลจะถูก decrypt ในเวอร์กสเตชันที่มันผ่านไปทำให้มีโอกาสที่ข้อมูลจะรั่วไหลได้

การป้องกันข้อมูลในระดับ transport layer จะดีกว่ามากเพราะข้อมูลจะไม่ถูก decrypt เมื่อมันวิ่งผ่านเวอร์กสเตชันตัวอื่น เป็นการลดความเสี่ยงได้มาก และไม่มีข้อเสียของการลดประสิทธิภาพของระบบด้วย เพราะมันจะไม่ต้อง decrypt ข้อมูลในทุก ๆ เวอร์กสเตชันที่ข้อมูลวิ่งผ่านไป

การป้องกันข้อมูลในระดับ application layer จะเป็นการป้องกันที่ดีที่สุด เพราะจะไม่ต้องไปแก้ไขโปรแกรมใน layer ใด ๆ เลยนอกจาก layer ที่เจ็ด layer อื่น ๆ ก็จะทำงานตามปกติและประสิทธิภาพของระบบก็จะไม่ตกลงเลย

การป้องกันระบบทางด้านฮาร์ดแวร์

ดังที่กล่าวมาข้างต้น คุณควรป้องกันทางด้านฮาร์ดแวร์ของระบบด้วย การป้องกันทางด้านฮาร์ดแวร์อาจแบ่งเป็นสองส่วนใหญ่ ๆ คือ การป้องกัน



ทางด้านฮาร์ดแวร์เองและการป้องกันข้อมูลโดยใช้เทคโนโลยีทางด้านฮาร์ดแวร์เข้าช่วย

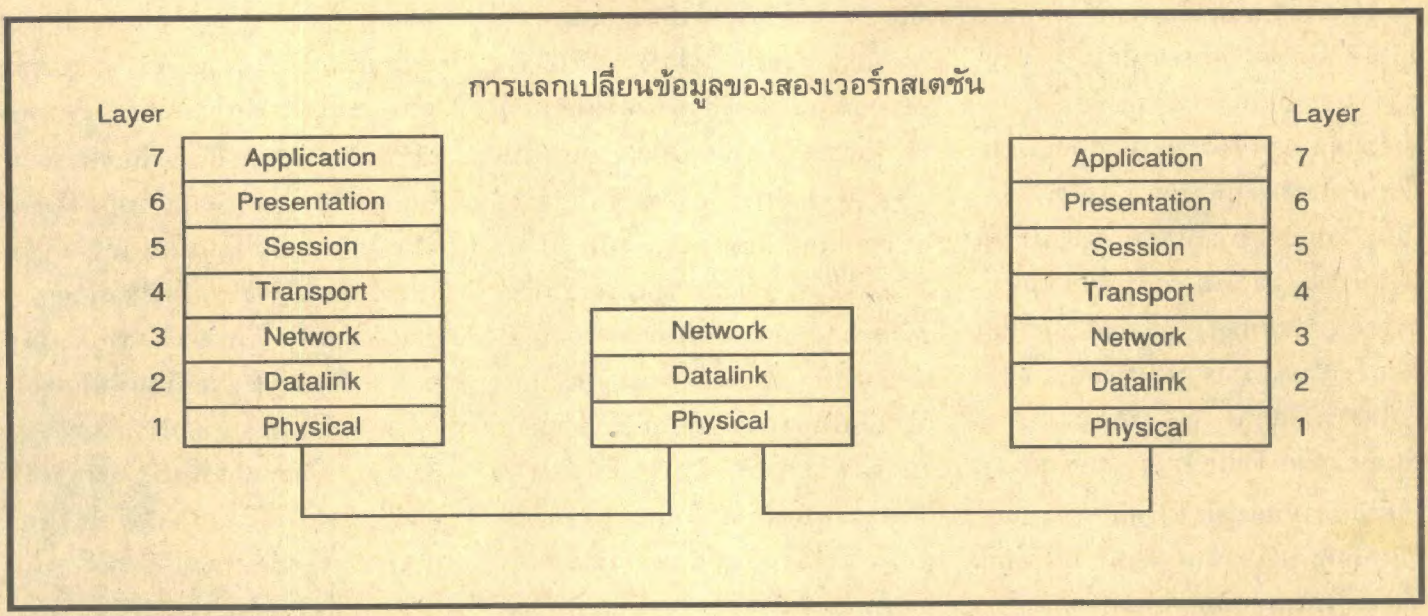
การป้องกันทางด้านฮาร์ดแวร์

คุณสามารถป้องกันทางด้านฮาร์ดแวร์ได้แก่ การป้องกันตัวเครื่องเซอร์ฟเวอร์ของระบบให้อยู่ในที่ ๆ ปลอดภัยจากภัยต่าง ๆ เช่น ไฟไหม้ น้ำท่วม หรือให้ห่างจากผู้ใช้ทั่วไป การเข้าถึงตัวเซอร์ฟเวอร์จะต้องมีการจดบันทึกหรือรับรู้โดยบุคคลอื่น ๆ ทุกครั้ง ในหน่วยงานที่ใหญ่ จะมีการสร้างห้องเฉพาะขึ้นมาเพื่อเก็บอุปกรณ์ทางด้านระบบทุกอย่างให้ปลอดภัย มีระบบป้องกันไฟ ระบบตรวจจับความร้อนและควันไฟ ระบบทำความเย็นและควบคุมความชื้น ระบบบัตรผ่านที่บันทึกชื่อและวันเวลาของผู้ที่จะเข้าไปทำงานในห้อง เป็นต้น

การป้องกันสายสัญญาณก็เป็นอีกอย่างที่คุณควรสนใจ การ encrypt ข้อมูลก่อนส่งไปมาในระบบเครือข่ายก็เป็นการแก้ปัญหาทางหนึ่งเท่านั้น แต่ถ้าคุณป้องกันไม่ให้ใครเข้ามาต่อเชื่อมเข้ากับระบบของคุณได้ จะเป็นการดีที่สุด ถ้าคุณใช้ระบบ star ในการวางสายคุณก็ควรจะต้องมีการจุดรวมสายอยู่ที่ใดที่หนึ่ง ซึ่งควรเป็นที่ ๆ บุคคลอื่นเข้าไปถึงได้ยาก สายสัญญาณส่วนใหญ่ที่วางจากจุดรวมสายควรจะอยู่ใต้พื้นหรืออยู่ท่อของสายสัญญาณ แต่ถ้าคุณยังใช้ระบบบัสอยู่ก็อาจจะยากซักนิดที่จะป้องกันสายสัญญาณ แต่ก็ยังสามารถทำได้โดยการร้อยสายเข้าในท่อซึ่งอยู่ระหว่างเวอร์กสเตชันแต่ละตัว

ฮับ (hub) ในปัจจุบันจะมีระบบการป้องกันผู้ไม่ประสงค์ให้เสียบสายสัญญาณเข้ากับมันได้โดยที่คุณสามารถกำหนดแอดเดรสของการ์ดแลนไปจำเพาะเจาะจงกับพอร์ตแต่ละพอร์ตของฮับ เมื่อมีผู้ต้องการจะเข้าต่อเชื่อมกับระบบเครือข่ายฮับจะตรวจสอบว่าเวอร์กสเตชันที่พยายามจะเข้ามาในระบบว่ามีแอดเดรสตรงกับที่กำหนดไว้กับพอร์ตนั้นหรือไม่ ถ้าไม่ตรงมันก็จะไม่ยอมให้เข้ามาในระบบได้พร้อมทั้งส่งสัญญาณเตือนไปให้ผู้ควบคุมระบบด้วย

ในระบบพีซีหรือระบบเครือข่าย การมีระบบการแบคอัพข้อมูลที่ดีก็จะสามารถที่จะนำเอาข้อมูลที่เสียหายกลับมาได้ การแบคอัพส่วนใหญ่จะอาศัยอุปกรณ์ที่เรียกว่า เทปแบคอัพ (tape backup) ซึ่งจะมีราคาถูกถ้าเทียบการเก็บข้อมูลด้านอื่น (เช่น เก็บในฮาร์ดดิสก์อีกตัวหนึ่ง เป็นต้น) อีกทั้งยังสามารถจัดเก็บข้อมูลได้เป็นจำนวนมากในตลับเทปหนึ่ง ๆ คุณอาจจะเก็บข้อมูลเป็นเวลานาน ๆ เป็นเดือนได้โดยใช้เทปเพียงไม่กี่ม้วนเท่านั้น ปัญหาบางอย่างของมันก็คือ จะใช้เวลานานพอสมควรทีเดียวในการจัดเก็บข้อมูลลงไปในเทป ที่ผู้เขียนเคยพบมาข้อมูลประมาณ 2 กิกะไบต์ อาจต้องใช้เวลาในการจัดเก็บถึง 2 ชั่วโมงทีเดียว ในระบบเมนเฟรม



รูปที่ 1 การป้องกันข้อมูลในระบบเครือข่าย

และระบบมินิคอมพิวเตอร์จะมีอุปกรณ์ที่สามารถจัดเก็บข้อมูลได้รวดเร็วกว่ามาก อีกทั้งการจัดเก็บข้อมูลลงเทปยังทำให้ตัวเซอร์ฟเวอร์ทำงานได้ช้าลงด้วย ดังนั้นการจัดเก็บส่วนใหญ่จะต้องทำตอนกลางคืนหรือเวลาที่ไม่ค่อยมีผู้คนใช้ระบบมากนัก

การป้องกันข้อมูลโดยใช้เทคโนโลยีทางด้านฮาร์ดแวร์เข้าช่วย

เป็นระบบ fault-tolerant ที่จะป้องกันข้อมูลที่อยู่ในฮาร์ดดิสค์ของคุณให้ปลอดภัย หรือเมื่อมีความเสียหายเกิดขึ้นคุณก็สามารถที่จะนำข้อมูลเก่านั้นกลับมาได้ ระบบที่ว่าจะเป็นการจัดการกับฮาร์ดดิสค์จำนวนมากของคุณให้มีพื้นที่เป็นผืนเดียวกันหมดซึ่งง่ายแก่การดูแลและจัดการ ระบบนี้เรียกว่า Redundant arrays of inexpensive disks หรือ RAID นั่นเอง

RAID แบ่งออกเป็นหกประเภท คือ

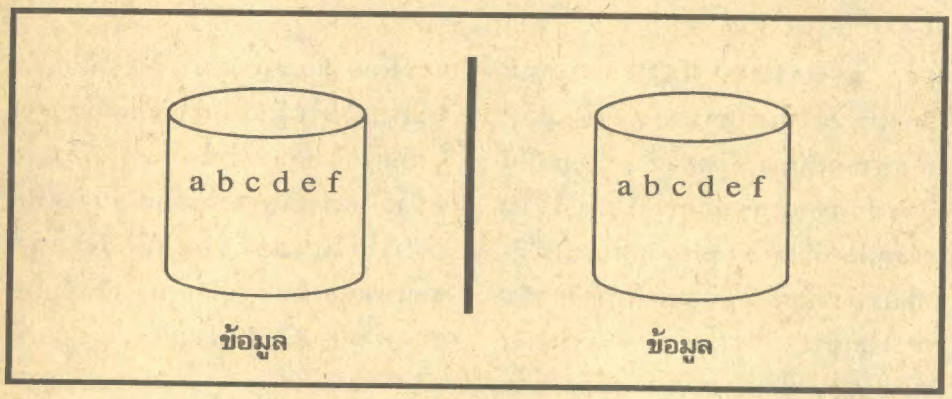
● **RAID 0 : RAID** ประเภทนี้จะไม่ช่วยให้เราสามารถนำข้อมูลที่เสียหายกลับมาใช้ใหม่ได้ มันจะเป็นการแยกข้อมูลของคุณไปเก็บไว้ในฮาร์ดดิสค์ที่แตกต่างกัน แต่ระบบปฏิบัติการจะเห็นมันเป็นฮาร์ดดิสค์เดียวกัน การแยกข้อมูลในฮาร์ดดิสค์เช่นนี้เรียกว่า striping เมื่อต้องการอ่านหรือเขียนข้อมูลลงไปหัวอ่านในแต่ละหัวในแต่ละฮาร์ดดิสค์ก็จะทำหน้าที่ในการอ่านหรือเขียนพร้อมกัน ทำให้การเข้าถึงข้อมูลมีความเร็วขึ้นมาก และมันก็สามารถใช้เนื้อที่ทั้งหมดของฮาร์ดดิสค์ได้

● **RAID 1 :** เป็นระบบที่เรียกว่า disk mirroring เป็นการแบ่งเนื้อที่ทั้งหมดของคุณออกเป็นสองส่วนเมื่อมีการเก็บข้อมูล มันก็จะถูกเก็บลงไปในดิสค์ทั้งสองส่วนนี้ ไฟล์แต่ละไฟล์ที่เก็บจะมีอยู่สองชุดด้วยกัน เมื่อข้อมูลเสียหาย มันจะดึงเอาข้อมูลที่อยู่อีกไดรฟ์หนึ่งมาใช้ทันที เป็นระบบที่มีความสามารถสูง มีความรวดเร็วในการเข้าถึงและดึงเอาข้อมูลออกมาใช้ ข้อเสียก็คือคุณสามารถใช้เนื้อที่ในฮาร์ดดิสค์ของคุณได้เพียงครึ่งเดียวเท่านั้น เพราะอีกครึ่งหนึ่งเป็นการเก็บข้อมูลที่เหมือนกันเพื่อนำมาใช้ในขณะที่ข้อมูลที่อยู่ในดิสค์ชุดแรกเสียหาย รูปแบบการเก็บข้อมูลของระบบ RAID 1 แสดงไว้ในรูปที่ 2

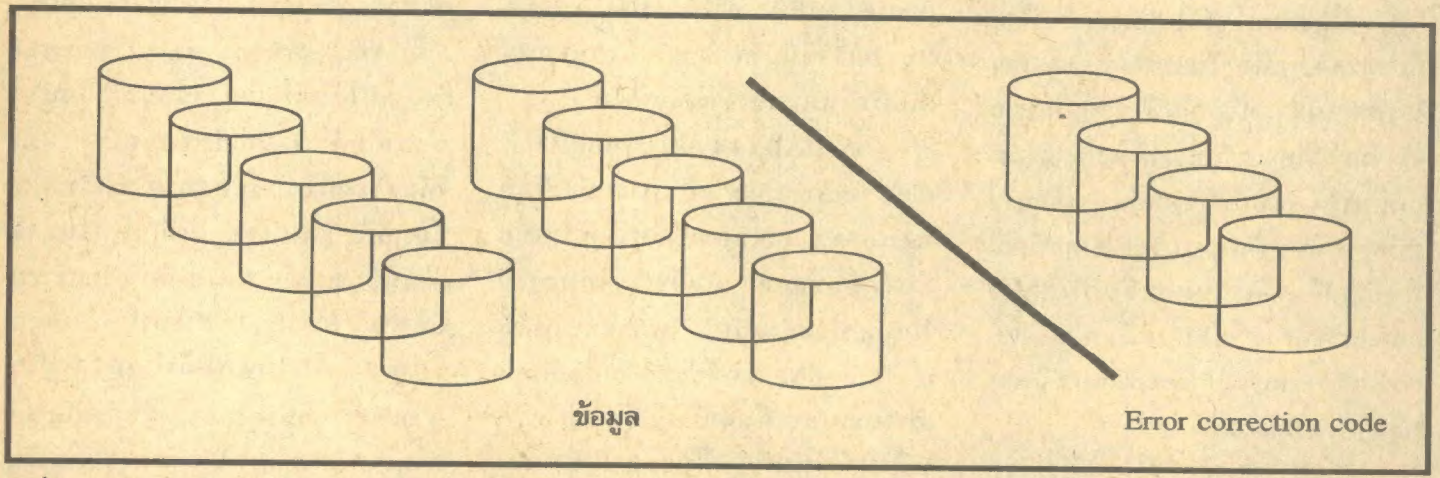
● **RAID 2 :** เป็นการปรับปรุงการทำงานของ RAID 1 ให้มีความสามารถและความเร็วที่สูงขึ้นโดยการตัดการทำ striping และการแยกเอาข้อมูลที่ใช้ในการแก้ไขข้อมูลที่เสียหายออกจากดิสค์ตัวที่เก็บข้อมูลมีการเก็บโค้ดการแก้ไขข้อมูลแทนที่จะเก็บเป็นข้อมูลอีกชุดหนึ่งทำให้มีเนื้อที่ในการเก็บข้อมูลมากขึ้นเมื่อเทียบกับระบบป้องกัน RAID 1 การอ่านหรือเขียนข้อมูลเข้าไปในดิสค์ก็ทำได้รวดเร็วกว่าเพราะหัวอ่านในฮาร์ดดิสค์แต่ละลูกสามารถอ่านข้อมูลได้พร้อม ๆ กัน ในขณะที่ใน RAID 1 มันจะต้องเขียน

ข้อมูลและโค้ดพิเศษในการแก้ไขข้อมูลไว้ในดิสก์ตัวเดียวกันทำให้กินเวลานานกว่า ในระบบนี้คุณสามารถใช้ฮาร์ดดิสก์ที่เก็บโค้ดพิเศษจำนวน 4 ตัวเพื่อเก็บข้อมูลในฮาร์ดดิสก์จำนวน 10 ตัว คิดเป็นความสามารถในการเก็บข้อมูลได้ประมาณ 70 เปอร์เซ็นต์ของเนื้อที่ฮาร์ดดิสก์ทั้งหมดดังรูปที่ 3 ข้อเสียก็คือในการเก็บข้อมูลจำนวนน้อย ๆ อาจทำให้ฮาร์ดดิสก์ทั้ง 14 ตัวของคุณทำการอ่านและเขียนข้อมูลจำนวนไม่กี่ไบต์นั้น (อย่าลืมว่ามันจะเห็นฮาร์ดดิสก์ทั้งหมดเป็นเนื้อที่ผืนเดียวกัน ดังนั้นไฟล์ไฟล์เดียวของคุณอาจเก็บอยู่บนฮาร์ดดิสก์ได้หลายตัว) ส่วนใหญ่จะไม่ค่อยมีใครใช้การป้องกันระบบ RAID 2 กันเท่าใดเพราะมันกินเวลาซีพียูของเครื่องเซอร์ฟเวอร์และเครื่องพีซีของคุณมากเกินไป

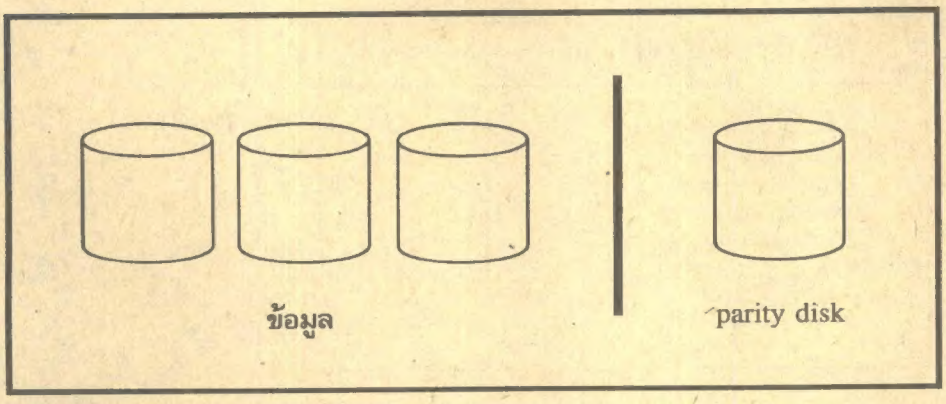
● **RAID 3 :** ได้ปรับปรุงการแก้ไขข้อมูลที่เสียหายให้ดีขึ้นใน RAID 2 จะใช้วิธีการแก้ไขข้อมูลที่เสียหายที่เรียกว่า bit-interleaving คือการเอาบิตต่าง ๆ ของแต่ละข้อมูลมาผสมกันเป็นโค้ดในการแก้ไขข้อมูลใน RAID 3 ไม่ได้ใช้วิธีการเหล่านั้นแต่หันมาใช้วิธีการใหม่เพื่อเก็บโค้ดในการแก้ไขข้อมูลมาไว้ในดิสก์ตัวเดียวที่เรียกว่า parity disk ถ้าข้อมูลในแต่ละบิต ไบต์ หรือ ไฟล์ ของคุณเกิดความเสียหาย ข้อมูลที่เก็บอยู่ใน parity disk จะถูกดึงออกมาเพื่อนำมาสร้างข้อมูลที่เสียหายนั้นกลับมาได้ ข้อเสียของระบบนี้ก็คือ จะมีการเขียนข้อมูลลงไปในฮาร์ดดิสก์มากเพราะมันไม่สามารถเขียนให้เสร็จสิ้นได้ภายในครั้งเดียว และการคำนวณ parity ก็จะกินเวลาของซีพียูด้วย ดังนั้นคุณควรเลือกดิสก์คอนโทรลเลอร์ที่มีความสามารถในการทำ parity ได้ก็จะช่วยได้มาก มันจะให้คุณเก็บข้อมูลได้ถึง 75 เปอร์เซ็นต์ของเนื้อที่ฮาร์ดดิสก์ทั้งหมด วิธีการป้องกันนี้เหมาะที่จะใช้ในเครื่องพีซีทั่ว ๆ ไป



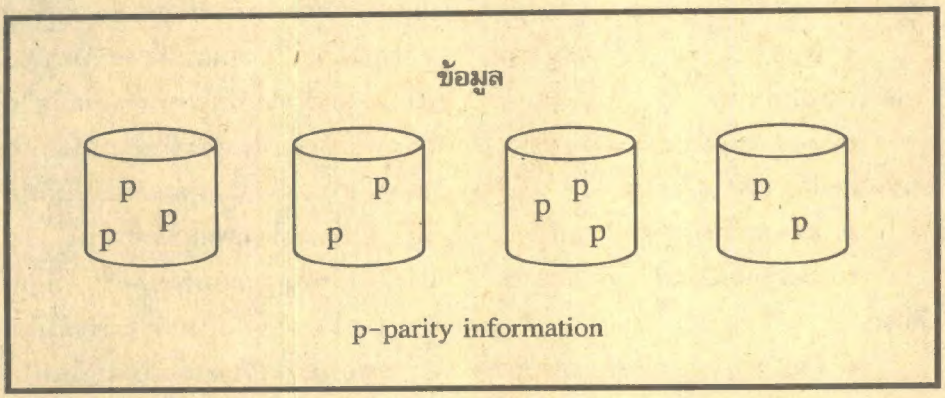
รูปที่ 2
การเก็บข้อมูลของ RAID 1 (disk mirroring)



รูปที่ 3 การจัดเก็บข้อมูลของระบบการป้องกัน RAID 2



รูปที่ 4
การเก็บข้อมูลในระบบ RAID 3



รูปที่ 5
ระบบการป้องกันแบบ RAID 5

ไม่เหมาะในการใช้กับเซอร์ฟเวอร์เพราะความเร็วของมันยังไม่ดีพอ รูปที่ 4 เป็นการแสดงถึงการเก็บข้อมูลของ RAID 3

● **RAID 4 :** หรืออาจเรียกว่า data guarding เป็นลักษณะการเก็บข้อมูลคล้ายกับ RAID 3 แต่เพิ่มความเร็วขึ้นมาก เพราะมันจะใช้ทำการคำนวณในระดับเซกเตอร์ แทนที่จะคำนวณในระดับบิตอย่างใน RAID 3 มันยังคงใช้ parity disk ตัวเดียวไม่เปลี่ยนแปลง การอ่านข้อมูลจะมีความเร็วกว่าการเขียนข้อมูลในการป้องกันแบบนี้ แต่ความเร็วโดยรวมของการอ่านและเขียนข้อมูลของ RAID 4 จะเร็วกว่า RAID 3 มากเพราะการคำนวณจะอยู่ในระดับเซกเตอร์

● **RAID 5 :** หรือเรียกว่า distributed data guarding การทำงานของมันจะไม่ใช้ parity disk เหมือนอย่างใน RAID 4 แต่มันจะวางข้อมูลของ parity ไว้ในดิสก์ที่เก็บข้อมูล ดังนั้นฮาร์ดดิสก์แต่ละตัวสามารถที่จะอ่านหรือเขียนได้พร้อมกัน โดยที่ไม่จำเป็นต้องรอการอ่านหรือเขียนข้อมูลจาก parity disk เลย เมื่อมีดิสก์ตัวใดเสีย ระบบยังคงสามารถทำงานได้อยู่ แต่อาจสูญเสียความรวดเร็วไปบ้างเพราะต้องมาคำนวณสร้างข้อมูลจาก parity information เมื่อดิสก์ที่เสียได้รับการเปลี่ยนแล้ว ข้อมูลต่าง ๆ ก็จะได้รับการคำนวณและสร้างขึ้นมาใหม่ วิธีการนี้จะทำให้การอ่านและเขียนข้อมูลเป็นไปได้อย่างรวดเร็วมาก แต่คุณต้องการดิสก์คอนโทรลเลอร์ที่มีความสามารถสูง (ซึ่งมีราคาแพงมากด้วย) คุณจะสามารถเก็บข้อมูลได้ถึง 85 เปอร์เซ็นต์ของเนื้อที่ฮาร์ดดิสก์ทั้งหมดที่คุณมีอยู่ การเก็บข้อมูลของ RAID 5 แสดงไว้ในรูปที่ 5

ระบบ RAID ที่นิยมใช้กันอยู่ในปัจจุบันคือ RAID 3 และ RAID 4 เพราะมีราคาค่อนข้างพอเหมาะในขณะที่ RAID 5 ที่มีราคาแพงสามารถป้องกันได้ดีและรวดเร็วกว่า RAID 5 กำลังเริ่มเป็นที่นิยมกันถึงแม้ว่ามันยังแพงอยู่ก็ตามเพราะ หลาย ๆ หน่วยงานเริ่มมีความเข้าใจในระบบการป้องกันข้อมูลมากขึ้นว่า ราคาที่แพงขึ้นของ RAID 5 จะช่วยให้พวกเขามีข้อมูลที่มีความมั่นคงสูงด้วยการตอบสนองที่รวดเร็วเป็นอย่างมาก

คอมพิวเตอร์ไวรัสคืออะไร

คอมพิวเตอร์ไวรัสคือซอฟต์แวร์ชนิดหนึ่ง ดังนั้นเครื่องคอมพิวเตอร์ของคุณสามารถโหลดซอฟต์แวร์ไวรัสขึ้นมาทำงานได้เหมือนกับซอฟต์แวร์ปกติชนิดอื่น ๆ แต่ต่างกันตรงที่ ไวรัสจะเข้ามาทำลายข้อมูลของคุณให้เกิดความเสียหายได้ และบางชนิดสามารถติดเข้าไปในแผ่นดิสค์ที่คุณใช้โดยคุณไม่มีทางรู้ตัวเลยถ้าไม่มีโปรแกรมป้องกันไวรัสช่วย ซึ่งแผ่นดิสค์นี้เมื่อนำไปใช้กับเครื่องคอมพิวเตอร์อื่น ก็จะทำให้ไวรัสไปติดกับเครื่องนั้น ๆ ด้วย

มีไวรัสมากมายหลายชนิดมากในปัจจุบัน แต่ละชนิดจะทำงานแตกต่างกัน บางตัวจะซ่อนตัวเองเข้าไปในไฟล์ executable และ boot sector บนเครื่องของคุณได้ มีไวรัสอยู่มากกว่า 1024 ชนิดในปัจจุบัน ตารางที่ 3 แสดงถึงข้อมูลคร่าว ๆ ถึงการติดไวรัสในระบบคอมพิวเตอร์ทั่ว ๆ ไป

จากที่กล่าวมาแล้วไวรัสเป็นสิ่งที่คุณไม่ต้องการในระบบอย่างแน่นอน เพราะมันสามารถทำลายข้อมูลในระบบได้เป็นอย่างดี เราควรหาทางป้องกันระบบของเราจากไวรัสในทุก ๆ ทาง

ลักษณะการติดของไวรัส	เปอร์เซ็นต์
Hard Drive Boot Record	2
Master Boot Record	2
Floppy Boot Sector	5
EXE files only	13
COMMAND.COM	16
Both COM and EXE files	24
COM files only	38

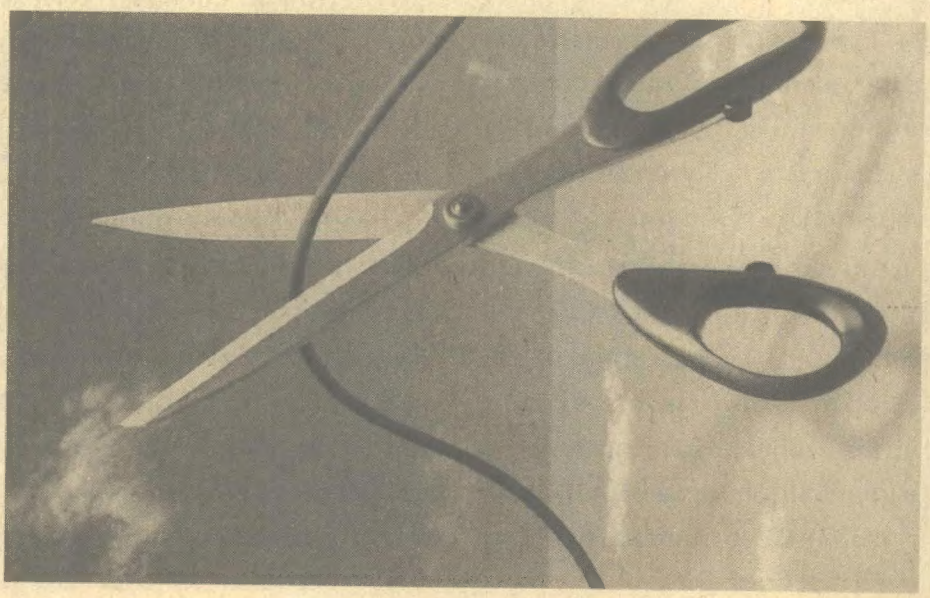
ตารางที่ 3
การติดของไวรัส

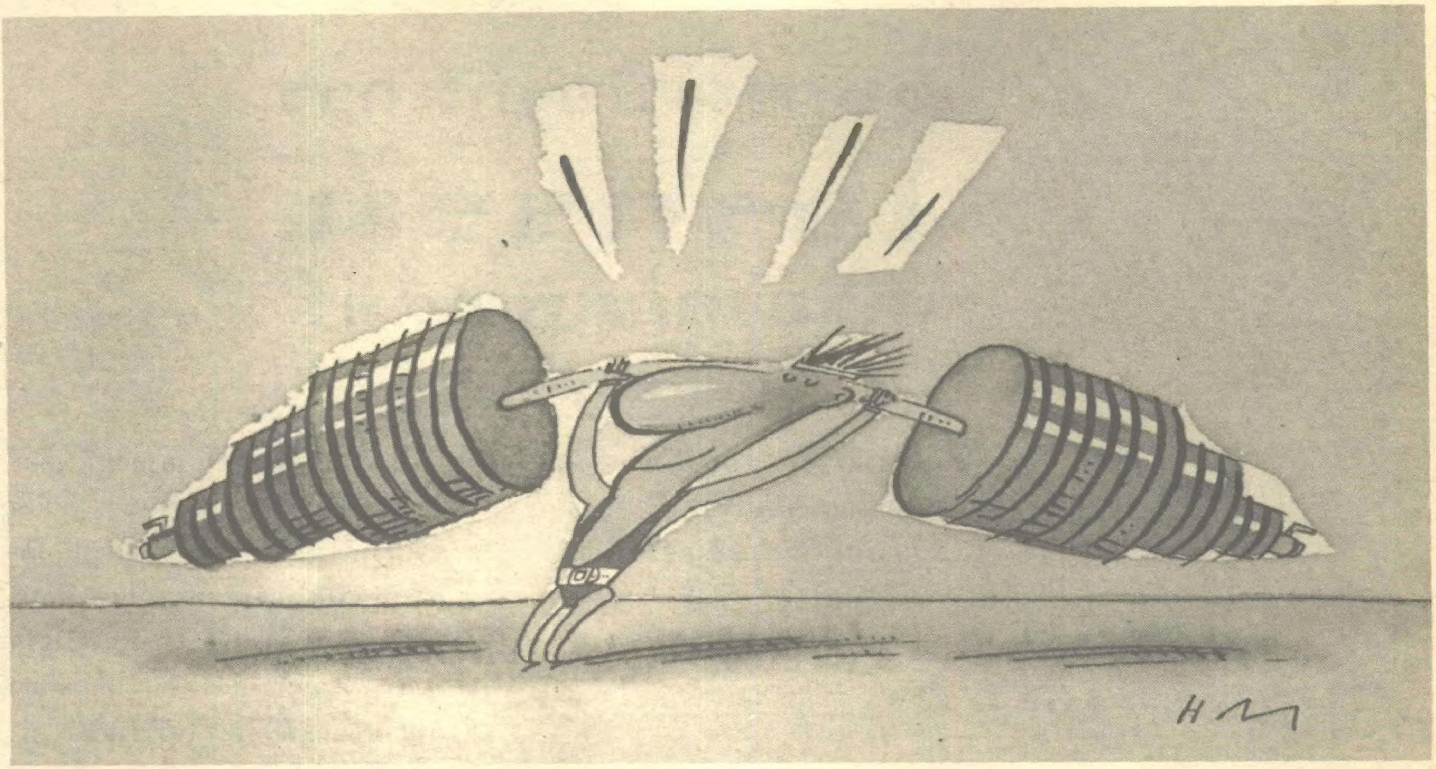
การป้องกันไวรัสเข้าในระบบ

เราควรมาดูกันก่อนว่าไวรัสเข้ามาในระบบเราได้ทางใดบ้าง ข้อมูลข้างล่างเป็นสาเหตุมากมายที่สามารถทำให้เครื่องของคุณหรือระบบของคุณติดไวรัสได้

- ติดจากแผ่นดิสค์ที่นำมาจากบ้าน
- ติดจาก BBS
- ติดจากแผ่นดิสค์ที่แจกฟรีในงานแสดง
- ติดจากแผ่นดิสค์ที่มาจากช่างซ่อมเครื่องหรือผู้ช่วยเหลือ
- ติดจากการดาวน์โหลดไฟล์มาจากระบบอื่น ๆ
- ติดจากแผ่นดิสค์ของแอพพลิเคชันซอฟต์แวร์ที่คุณซื้อมา
- ติดจากแผ่นดิสค์ของลูกค้า
- ติดจากแผ่นดิสค์ที่มาจากสถานศึกษา
- ติดมากับเครื่องพีซีที่คุณซื้อมา
- ติดจากระบบเครือข่าย
- ฯลฯ

จะเห็นได้ว่าการติดไวรัสส่วนใหญ่มาจากแผ่นดิสค์นั่นเอง ดังนั้นการป้องกันไวรัสที่ดีจะต้องมีการตรวจสอบแผ่นดิสค์ทุกแผ่นที่จะนำมาใช้กับเครื่องของคุณด้วย ไม่ว่าแผ่นดิสค์แผ่นนั้นจะมาจากใครก็ตามที่คุณเห็นว่าเชื่อถือได้ หรือแม้แต่ซอฟต์แวร์ที่คุณเพิ่งจะแกะกล่องก็อาจจะมีไวรัสติดมากับแผ่นดิสค์ได้ ปัจจุบันมีซอฟต์แวร์ต่อต้านไวรัสมากมายในตลาดคอมพิวเตอร์ ที่คุณสามารถโหลดเข้าไปในเครื่องซึ่งมันจะตรวจสอบหาไวรัสจากแผ่นดิสค์ทุก ๆ แผ่นที่คุณจะใช้ หรือไฟล์ทุก ๆ ไฟล์ที่คุณกำลังจะโหลดขึ้นมาใช้งานว่าติดไวรัสหรือไม่ พร้อมทั้งมีซอฟต์แวร์แก้ไขไฟล์ที่มีการติดไวรัสให้ด้วย





แต่คุณก็จำเป็นต้องอัพเกรดซอฟต์แวร์การตรวจจับไวรัสบ่อย ๆ ด้วยเพราะมีไวรัสเกิดใหม่อยู่ตลอดเวลาซึ่งพัฒนาขึ้นมาเพื่อหลบหลีกการตรวจจับได้

การเตรียมแผนฉุกเฉิน

ไม่ว่าข้อมูลของคุณจะเสียหายอย่างไร หรือโดยใคร การเตรียมแผนการฉุกเฉินที่ดีก็จะทำให้ความเสียหายอันนั้นน้อยลงไปได้ เช่น การเก็บชิ้นส่วนของฮาร์ดแวร์บางชนิดเอาไว้ เพื่อทำการสับเปลี่ยนเมื่อมีความผิดพลาดทางฮาร์ดแวร์เกิดขึ้น หรือทำการตกลงกับผู้ขายให้เตรียมอุปกรณ์บางชนิดไว้เพื่อสับเปลี่ยนเมื่อมีความจำเป็น

จากประสบการณ์ของผู้เขียนเอง ผู้ซื้อควรทำสัญญากับผู้ขายตั้งแต่ตอนซื้อไว้เลยว่า จะมีการแก้ไขหรือเปลี่ยนอุปกรณ์ฮาร์ดแวร์บางชนิดถ้ามันชำรุดเสียหายในเวลาที่กำหนดไว้ ในระบบที่สำคัญมาก ๆ ผู้ควบคุมระบบนอกจะต้องหาทางป้องกันความเสียหายแล้วก็ควรจะต้องมีแผนรับมือกับเหตุการณ์ที่ไม่คาดฝันไว้ด้วย เช่น มีการเก็บข้อมูลในเซอร์ฟเวอร์ทั้งหมดจากเทปแบคอัพและนำเทปข้อมูลเหล่านั้นไปเก็บไว้นอกสถานที่เมื่อเกิดเหตุการณ์อันที่จะทำให้เซอร์ฟเวอร์หรือห้องเก็บเซอร์ฟเวอร์ทั้งหมดเสียหาย (เช่น ไฟไหม้ เป็นต้น) ผู้ควบคุมระบบก็ยังสามารถเอาข้อมูลทั้งหมดที่อยู่ในเทปมาโหลดใส่เครื่องเซอร์ฟเวอร์ฉุกเฉินที่เตรียมไว้แล้ว และสามารถทำให้ระบบดำเนินต่อไปได้ ถึงแม้ว่าบางครั้งจะไม่ทั้งหมดเลยก็ตาม

แผนฉุกเฉินจะทำได้อย่างมีประสิทธิภาพและครอบคลุมในเหตุการณ์ได้มาก ก็ด้วยความรอบคอบของผู้วางและควบคุมระบบ ซึ่งควรมีการพิจารณาถึงความเป็นไปได้และทางแก้ไขต่าง ๆ ในหน่วยงานใหญ่ ๆ หลายแห่งแผนฉุกเฉินนี้จะต้องมีการศึกษากันก่อนที่จะมีการติดตั้งระบบจริง ๆ เพื่อเป็นการป้องกันระบบให้ทำงานได้อย่างไม่ติดขัด

บทส่งท้าย

การป้องกันระบบไม่ใช่เป็นงานของผู้วางระบบ หรือผู้ควบคุมระบบเท่านั้น ผู้ใช้ทุกคนที่ใช้งานในระบบจะต้องช่วยเหลือในการป้องกันด้วย ความสำคัญของมันมีมากกว่าที่ผู้ใช้ส่วนใหญ่จะสนใจมากนัก ดังนั้นคุณควรจะต้องให้การศึกษาแก่ผู้ใช้ระบบทุกคนให้เข้าใจถึงความสำคัญของมันและวิธีในการที่ผู้ใช้จะช่วยในการป้องกันระบบด้วย การป้องกันที่ได้ไม่เพียงแต่ทำการป้องกันทางด้านฮาร์ดแวร์หรือซอฟต์แวร์เท่านั้น แต่มันหมายถึงการพัฒนาให้ผู้ใช้มีความสามารถในการป้องกันระบบเมื่อนั้นคุณก็จะรักษาระบบให้มีความปลอดภัยได้อย่างดีเยี่ยมทีเดียว